Sustainable, Reliable Mission-Systems Architecture

Graham O'Neil,* James K. Orr, † and Steve Watson‡
United Space Alliance, Houston, TX, 77058

A mission-systems architecture, based on a highly modular infrastructure utilizing open-standards hardware and software interfaces as the enabling technology is essential for affordable and sustainable space exploration programs. This mission-systems architecture requires (a) robust communication between heterogeneous systems, (b) high reliability, (c) minimal mission-to-mission reconfiguration, (d) affordable development, system integration, and verification of systems, and (e) minimal sustaining engineering. This paper proposes such an architecture. Lessons learned from the Space Shuttle program and Earthbound complex engineered systems are applied to define the model. Technology projections reaching out 5 years are made to refine model details.

I. Introduction

The mission systems architecture to support ambitious space exploration activities will be challenged at the physical level by large scale distances and hostile environements, at the local level by allocation constraints, and at the support level by organizational, social and cultural divides. Each of these except for the long distances and hostile environement will change on a periodic basis several times over the decades of space exploration envisoned by the NASA Roadmap [1]

The paper will present four operationally significant criteria that will be used in defining the systems and in allocating functions for local or remote performance. Three major components to be examined for their contribution to deploying a successful mission systems architecture are:

- A hardware layer based on a node-based network with tunable redundancy, automated fail-over based on intelligent agents, and plug and play interaction that includes automatic reconfiguration based on detection and recognition of new components.
- A software architecture applicable from the lowest level subsystem to the integrated mission system based on open-standards middleware, eg IEEE 1516.
- A transparent switching framework of flight hardware, flight equivalent hardware, emulation of flight hardware, and network-connected computers containing high-fidelity software models as well as stubs and harnesses necessary for system testing.

II. The Four Keys to Success of Mission System Architecture

"A central concept of the new U.S. National Vision for Space Exploration is that space exploration activities must be 'Sustainable'" (NASA's 2004 H&RT Formulation Plan). Sustainability encompasses the following four key areas that are critical to successful deployment and operations of the conceptual mission systems architecture. Each of these criteria has built-in trades that if carried out consistently and systematically will lead to an implementation that supports human space exploration for decades to come.

- Affordable: Life cycle costs at each stage must be consistent with NASA budgets. Unplanned spikes must be minimized. Future costs resulting from decisions made today should be well grounded with relevant validation and historical basis. The primary trade is when will a system or capability be available and in what quantity.

---

* Computer Scientist, Shuttle Flight Software, 600 Gemini M/C USH-632L, AIAA Senior Member.
† Chief Engineer, Shuttle Flight Software, 600 Gemini M/C USH-631A, Member
‡ Computer Scientist, Shuttle Flight Software, 600 Gemini M/C USH-635L

- Reliable and safe: Future space exploration systems, infrastructures and missions must be safe and reliable. Safety will be defined as "As Safe As Reasonably Achievable" (ASARA); analogous to the nuclear industries "As Low As Reasonably Achievable" (ALARA) when deciding on alternatives involving human exposure to radiation.

- Effective: The capabilities of a new system or infrastructure must be worth the costs of developing, building, and owning them. The goals and objectives achieved by missions using those systems and infrastructure components must be worth the costs and risks of owning them.

- Flexible: The families of new systems, infrastructures, and technologies should be capable of adapating to changing policy objectives, requirements, interfaces, and operational scenarios. The systems and infrastructures whould be capable of extension to support new missions. The principal focus of trades in this area is how much flexibility is desired in each component of the MSA.

The three MSA Components treated in this paper support the four operations criteria as explained below:

Affordability
- Transparent switching significantly reduces costs by supporting new systems concept validations earlier without real hardware, by reducing hardware requirements for training scenarios, and by reducing systems integration efforts.
- Reliable automatic reconfiguration required in long distance missions, virtually eliminates expensive ground-based reconfiguration applications and reduces human-in-the-loop interaction requirements for shorter range missions.
- Incremental building block approach simplifies integration of new systems into existing flight systems.

Reliability/Safety
- Redundancy tuned to the level required, whether N+1, N+M or full duplication where necessary, to give quantifiable probability of mission success.

Effectiveness
- Building upon recognized industry/space standards significantly reduces costs and the risk of development while offering a highly effective combination of real-time performance, scalability, and fault-tolerance.

Flexibility
- Open-standards interfaces allow for technology evolution.
- Plug and Play supports the building block approach.
- Automated reconfiguration driven by intelligent agents provides fast responses with minimal human demand.

III. Where Are The Challenges?

Technical challenges are expected in providing the scalability required for increasingly more ambitious space missions. Advancing technology can be counted on up to a point. Robust margins are helpful, but must be paid for in advance with no guarantee thay will be used.

Automatic reconfiguration and the plug and play implementation require strict adherence to standards. Making the standard interface infrastructure robust enough to minimize the need for unique interfaces is a technical challenge to be addressed. But much of the risk has been reduced by DOD and industry initiatives in High Level Architecures (HLA) . Re-use of these HLAs eliminates major overhead of developing such an infrastructure from scratch. So work can be focused on interfacing with common HLA interfaces rather than painful iterative refinement of another standard exclusive to the space community.

Reconfiguration work must begin early so that major cost drivers such as number of modes and states, interfaces, and size of the data and information base will be accurate. Addition of a mojor mode late in the development cycle will have adverse effects on cost and scheduel while increasing program risk. Early definition of these features provides a solid foundation for mission system planners and analysts to begin scenario development and analysis.

This early start can be leveraged to gain much experience in safety related issues while there is still time to accommodate changes.

Each generation of aerospace modeling and simulation faces new challenges since data becomes more refined, CPUs run faster, and smaller details become important in second order interactions. Other difficulties cease to be a problem. No one develops Six Degree of Freedom simulations in Assembly language to fit CPU provisions anymore. But no one has a solid answer to automated reconfiguration requirements for life critical functions on very long term space missions.

Based on recent experience, modeling and simulation approaches should utilize:

A. Tight coupling between the operational software, and that used for test, and training.
B. Tight coupling of the simulators with the operational software.

Based on need projections for long duration space missions, new start modeling and simulation approaches should include:

A. Use of mirrored networks for operational and simulations.
B. On-board versions of the simulations for checkout, training, test, and procedures development.

IV. Future Vision

Modeling and simulation will play an important role in the development of new space systems. The development and use of the models and simulations will have significant impact on cost and schedule, so it is important to provide the best framework and tools. Models will be used for early prototype validation, for flight and support software development, for hardware checkout, and for crew and ground support training. A continuing challenge is the accurate emulation of hardware by the models. To minimize cost, the models should be developed once and reused, as required, throughout the various mission phases: planning, preparation, flight, and post-mission analysis.

One way to reduce simulation costs is to factor the need for models into the hardware architecture for the envisioned space vehicle. Considering the operational aspects during hardware design will avoid the need for the parallel modeling systems and additional overhead prevalent in today's operations using custom models or simulations at each facility or lab. An architecture that supports generic hardware executing models and using the same interfaces as the real hardware allows the models to be used earlier and more effectively in the development and operational support of the next generation space vehicles. For example, a model of a proposed hardware upgrade can be developed and used within the existing vehicle architecture to better determine the impacts to the overall system before the actual hardware specifications are released.

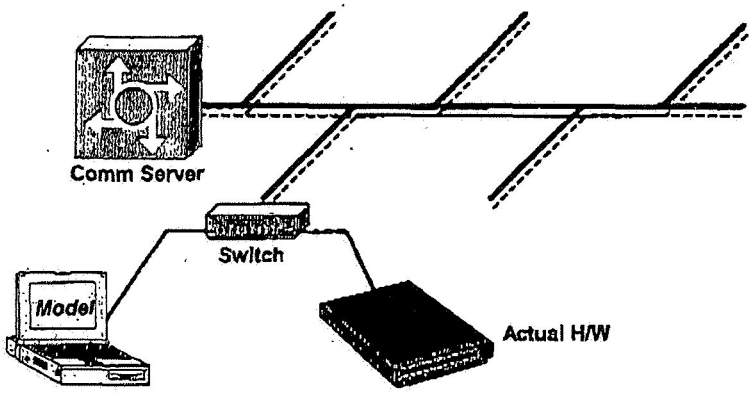

Figure 1. Model Insertion In Operational System

The entire space vehicle's systems would be set up as a high-speed interconnected system of networks. Each system (engines, environmental, maneuvering, landing gear, displays, flight control computer, mass memory, telemetry, etc) would have its own logical computer resources. The redundant network would provide communications, centralized timing, and power capability for each system. All flight hardware would be designed

and certified to endure a lengthy space mission. Figure 2 shows the main features of the hardware components of the architecture.

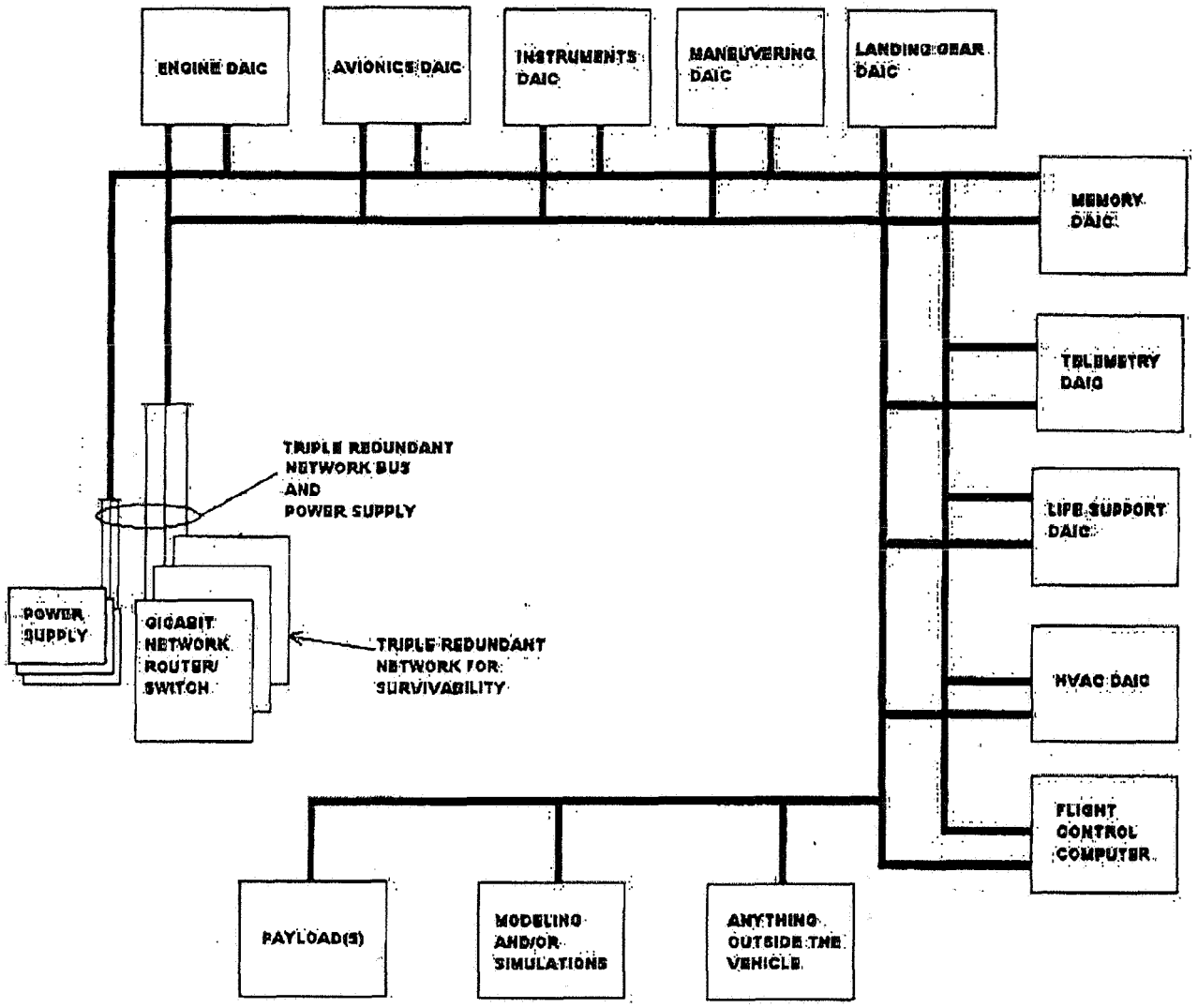

Figure 2. Notional Space Exploration Mission Architecture

Several commercial vendors build network switches and routers that operate at up to 10 billion bits per second data transfer rates. The spacecraft's network would be built around these high-speed network switches. The network would be triple-redundant (as on the B2 Bomber or Space Shuttle) for survivability. For a sizing example: each system would require 3 IEEE 802.3ak gigabit Ethernet cards. The 10-gigabit standard is the newest and the fastest standard; future network bus speeds will be faster. Why is this bandwidth required? It allows essentially real-time operations and can be easily upgraded. Most current aerospace systems have a bandwidth constraint that hampers insertion of additional components or development of new functions. Current generation architecture does not provide the bandwidth required to efficiently upgrade the vehicle. So additional parallel paths, a fast track qualification effort for special purpose hardware, and a COTS hardening effort for Firewire or Spacewire data transport will provide the added robust margins.

The network would also provide the ability to use generic testing hardware (e.g., portable laptop computers using standard spacecraft network interface connectors) to simulate any hardware system. Since this is a network, these

could be either inside the vehicle or external to the vehicle. Models and/or simulations, or anything outside of the vehicle would plug into the network through common network connectors.

Table 1 summarizes some of the key benefits of the component model based network approach. By interconnecting systems via a common communications pathway, we avoid some of the maintenance and upgrade problems that exist today. Having each system as an independent element with plug and play capability enables

A. Upgrading of any system without disabling the other systems
B. Support for a heterogeneous hardware environment.
C. Reduced maintenance downtime – replaces or upgrade, as required

Table 1. Key Benefits of Component Model Networks

1. Reduces maintenance downtime
2. Simplifies upgrades of systems. To "plug into" the network, the new system would have to meet the IEEE 802.3ak Gigabit Ethernet standard
3. Reduced weight due to fewer components
4. Easier to isolate and troubleshoot problems
5. Supports a heterogeneous hardware environment
6. Reduced development and sustaining costs

Each Data Acquisition, Instrumentation and Control (DAIC) should be developed to support various modes of operation. Looking at today's current environment, you can see considerable cost is involved in simply providing an environment that supports simulations for upgrading the system and for providing the training required to support space missions. Table 2 briefly describes the five modes that should be supported.

Table 2. Modes of Operation

Mode of Operation	Description
Normal	The system performs normal operations activities (polling, communications, etc.)
Simulator	• A specified system suspends activities to allow a simulator scenario to be performed. • Systems could be set to mimic another vehicle (similar to SAIL). – Similar to the FB-111 and B2 Bomber that have the ability to simulate missions on the ground
Independent	Each system could be run totally independent of the rest of the ship's systems.
Emergency	Each system could have a minimal back up program that would enable it to take charge of the entire ship in case of emergency. In this mode, each system computer would be capable of becoming the backup Flight Control Computer.
Super	Links all the vehicle's computers together to solve high-powered computational tasks. This mode of operation could also be used for more sophisticated high-powered simulations.

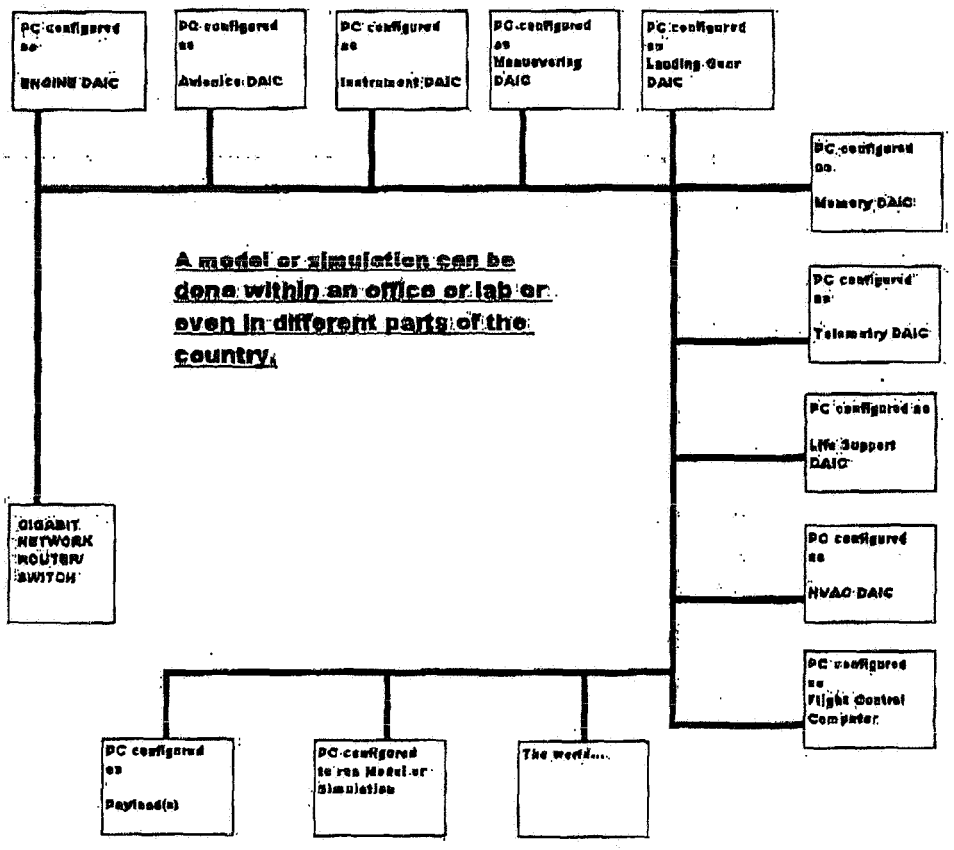

Figure 2. Network Concept Integrating Any-Source Simulations

The use of a standard network, based on Internet technologies, provides the capability to perform the following from any workstation(s):

- A simulation or construction of a model of the entire ship's system (reference Figure 2-3)
- Execution of a mission simulation
- Advance testing of reconfigurable measurands and systems from the office environment.

Sustainable space exploration requires more reliable and adaptable systems, particularly for missions with significant component degradation such as lunar robots or for prolonged missions like JIMO. Traditional systems, which provide redundant components improve robustness, but increase complexity, are costly, and provide limited adaptability. In contrast, modular architectures provide sustainability through reconfigurable component designs. To reap the maximum benefit from such architectures, intelligent adaptive software must be combined with modular designs to provide inexpensive, reliable, and reconfigurable space platforms which are self-configuring, self-maintaining and self-healing. The combination of intelligent adaptive software and modular architectures impacts NASA at the by endowing any design incorporating such technologies with improved sustainability.

Recent advances in multi-agent coordination methods may be leveraged to maximize system-wide sustainability by treating subsystems within the architecture as agents. When subsystems fail or mission goals change, adaptive agents representing the subsystems compensate by reconfiguring the parameters of, and interactions between, sub-systems. Such compensations minimize the need for expensive human intervention, and can adapt in a timely fashion in time-critical scenarios when there are long communication delays. Additionally, by including humans as additional agents in the multi-agent system, variable levels of autonomy may naturally be supported. Further, because the system is distributed across agents (systems) there is no need for centralized control, and scalability is

excellent. Generic reconfigurable, distributed, adaptable multi-agent-based architectures may be applied to movement control systems on lunar robots, to power or propulsion systems, to life support systems, or to any system that is susceptible to degradation or re-tasking.

V. Key operational aspects

One of the biggest obstacles to overcome is the ability to stop multiple models concurrently. This capability is required to support checkpoint/restart so that the whole environment can be saved at some specific point in time and then restarted later. This is especially beneficial during software development and during training. It is not feasible to run all the various components until they reach the specific point each time you want to test or train. Concurrent halts are also required to allow snapshots or dumps to be taken for analysis.

Another big hurdle is the introduction of malfunctions into the model so off-nominal scenarios can be reproduced and investigated. If the program has a robust reconfiguration process, then that process could be used to help determine the operational limits.

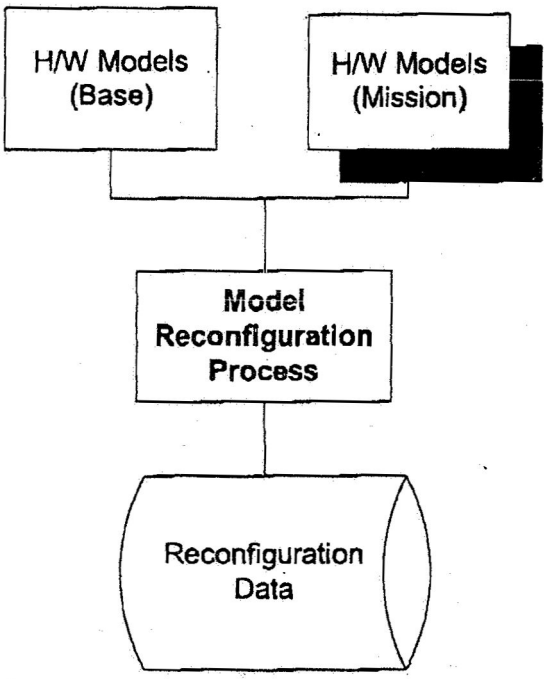

Figure 3. Model – Reconfiguration Link

VI. Recommendations

As described in the paper, there are a multitude of options available. The selection of the approach to take for modeling software is based on the selection of the processing capabilities required in each system. This includes the onboard as well as ground systems.

The key point here is to closely tie the selection of modeling software to the architecture decisions. This will significantly reduce the need for "point solutions" that have driven up the operational costs in the current shuttle program.

The development and demonstration of a prototype simulation harness with a limited set of vehicle software would provide insight and definition of simulator requirements, design, instrumentation strategies, and the target vehicle network.

The basic framework for a robust, high capacity network supporting multiple simultaneous modes of operation has presented in this paper. The use of an internet-based network tied with common interfaces allows the basic avionics framework to be used anywhere, anytime. It reduces the need to have specialized flight-like hardware, except where actually required. It also supports the concept of allowing work to be performed from multiple

locations. Teleworking is just one example that comes to mind. It also has significant benefits for the Mission Evaluation Room (MER) and for the MCC.

The separation of vehicle operation data from payload data is strongly encouraged. The changing needs for payload data forced the SSP to develop perform mission-to-mission reconfiguration processes. Since we had to perform a reconfiguration for each mission, this lead to additional operational changes being accepted since we had to "do a reconfiguration anyway." This should be avoided. This separation actually supports the vision for a spacecraft with multiple configurations, similar to the SpaceLab. The separate payload network would exist only in the payload module and it could connect to a central communications server that provides required data wherever needed.

One of the traditional requirements for space hardware was that it must be deterministic. If you have a network protocol with the potential for network collisions, how do you determine latency? How can you ensure that the network does not get overloaded? Suppose a hardware component malfunctions and begins to overload the network. How do you address that situation?

These questions need to be answered. These are problems that are being dealt with today. But they do need to be addressed early so sufficient maturity can be provided in the design solution.

VII. Conclusion

The successful development and demonstration of this architecture will have a "system-of-systems level impact" on future space-exploration missions. Major benefits include

- Significant reduction in development and sustaining costs of system development, integration, verification, and reconfiguration.
- Tunable redundancy and understandable interfaces for improved reliability.
- Flexible and effective open standards that are industry compatible supporting technology evolution.
- Enable embedded just-in-time in-flight training
- Direct applicability to surface-based facilities.